BEST AVAILABLE IMAGES

Defective images within this document are accurate representations of the original documents submitted by the applicant.

Defects in the images may include (but are not limited to):

- BLACK BORDERS
- TEXT CUT OFF AT TOP, BOTTOM OR SIDES
- FADED TEXT
- ILLEGIBLE TEXT
- SKEWED/SLANTED IMAGES
- COLORED PHOTOS
- BLACK OR VERY BLACK AND WHITE DARK PHOTOS
- GRAY SCALE DOCUMENTS

IMAGES ARE BEST AVAILABLE COPY.

As rescanning documents *will not* correct images, please do not report the images to the Image Problem Mailbox.

(12) INTERNATIONAL APPLICATION PUBLISHED UNDER THE PATENT COOPERATION TREATY (PCT)

(19) World Intellectual Property Organization
International Bureau

(43) International Publication Date
22 March 2001 (22.03.2001)

PCT

(10) International Publication Number
WO 01/20463 A1

(51) International Patent Classification[7]: G06F 12/14, 1/00, H04L 29/06

(21) International Application Number: PCT/SE00/01811

(22) International Filing Date:
18 September 2000 (18.09.2000)

(25) Filing Language: Swedish

(26) Publication Language: English

(30) Priority Data:
60/154,395 17 September 1999 (17.09.1999) US
0001687-3 5 May 2000 (05.05.2000) SE

(71) Applicant *(for all designated States except US)*: **FINGLOQ AB** [SE/SE]; Banehagsliden 5, S-414 51 Göteborg (SE).

(72) Inventors; and
(75) Inventors/Applicants *(for US only)*: **MARTINSSON, Roy** [SE/SE]; Laxgatan 1D, S-426 79 Västra Frölunda (SE). **ANDLER, Oskar** [SE/SE]; Furugatan 1, S-413 21 Göteborg (SE).

(74) Agent: **GÖTEBORGS PATENTBYRÅ DAHLS AB**; Sjöporten 4, S-417 64 Göteborg (SE).

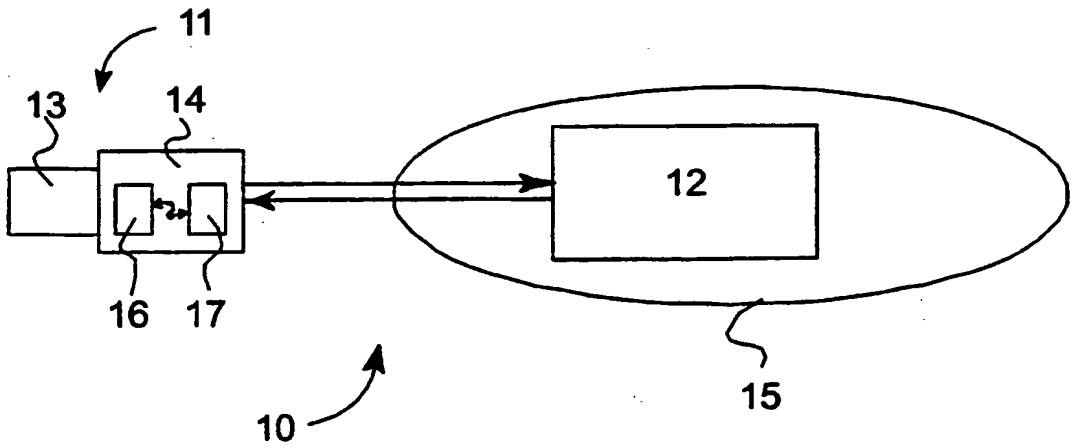
(81) Designated States *(national)*: AE, AG, AL, AM, AT, AT (utility model), AU, AZ, BA, BB, BG, BR, BY, BZ, CA, CH, CN, CR, CU, CZ, CZ (utility model), DE, DE (utility model), DK, DK (utility model), DM, DZ, EE, EE (utility model), ES, FI, FI (utility model), GB, GD, GE, GH, GM, HR, HU, ID, IL, IN, IS, JP, KE, KG, KP, KR, KR (utility model), KZ, LC, LK, LR, LS, LT, LU, LV, MA, MD, MG, MK, MN, MW, MX, MZ, NO, NZ, PL, PT, RO, RU, SD, SE, SG, SI, SK, SK (utility model), SL, TJ, TM, TR, TT, TZ, UA, UG, US, UZ, VN, YU, ZA, ZW.

(84) Designated States *(regional)*: ARIPO patent (GH, GM, KE, LS, MW, MZ, SD, SL, SZ, TZ, UG, ZW), Eurasian patent (AM, AZ, BY, KG, KZ, MD, RU, TJ, TM), European patent (AT, BE, CH, CY, DE, DK, ES, FI, FR, GB, GR, IE, IT, LU, MC, NL, PT, SE), OAPI patent (BF, BJ, CF, CG, CI, CM, GA, GN, GW, ML, MR, NE, SN, TD, TG).

Published:
— *With international search report.*
— *Before the expiration of the time limit for amending the claims and to be republished in the event of receipt of amendments.*

For two-letter codes and other abbreviations, refer to the "Guidance Notes on Codes and Abbreviations" appearing at the beginning of each regular issue of the PCT Gazette.

(54) Title: SECURITY ARRANGEMENT



(57) Abstract: The present invention relates to a security arrangement (10) for ensuring access to a unit or information in a unit, mainly comprising a key unit (11) and a lock unit (12). The key unit (11) is arranged in a distance from the lock unit comprising an input unit (13) and a communication unit (14). The identification of a user is performed in the key unit (11) before the lock unit accepts locking/unlocking.

WO 01/20463 A1

Title

SECURITY ARRANGEMENT

TECHNICAL AREA

The present invention relates to a security system for securing a unit or a set of information.

DESCRIPTION OF STATE OF THE ART

The increasingly rapid development within the electronics area has resulted in more electrical apparatuses with reduced size and mobility. The mobility itself has lead to, not only the apparatus itself but also the information stored therein have become appealing and attractive for thieves.

The known security arrangements provide either locking using hardware or software in combination with a primary input signal.

In the case of hardware lock, a first input unit is used, e.g. fingerprint input (a biometric sensor), pin-code combined with or without an additional unit, e.g. a so-called smart-card or the like.

In the software case a verification software is used, which controls that a correct input (pin-code, fingerprint etcetera) is presented via an external input unit. Normally, the software is installed in a storage unit, such as a hard disc, which is easily accessible.

SUMMARY OF THE INVENTION

The object of the present invention is to provide a very reliable and safe device for preventing access to equipment and/or information stored therein.

Another object of the present invention is to provide a device, which can be combined with different units, both for locking and identity input.

One of the advantages with the arrangement, according to the present invention, compared to known technique, is amongst others that (if applicable in a computer) no modifications of the operating system or the BIOS of the computer are needed. The fact is that such systems are easy to force, even without any greater knowledge within the area.

Furthermore, a lock unit, according to the invention, is integrated in the equipment to be protected, implying a complete safety, besides that the normal inputs and outputs of the equipment, ports, etc., do not need to be modified.

These objects have been achieved by means of the security arrangement for securing access to a unit or information in a unit, comprising mainly a key unit and lock unit, which is characterized in that the key unit is arranged in a distance from the lock unit comprising an input unit and a communication unit, and that the identification of a user is carried out in the key unit before locking/unlocking is accepted by the key unit.

BRIEF DESCRIPTION OF THE DRAWINGS

In the following, the invention will be described with reference to the embodiments according to the enclosed drawings, in which:

Fig.1 shows a block diagram over main parts of an arrangement according to the invention,

Fig.2 shows a diagram over the communication between two units in the arrangement according to the invention,

Fig. 3 shows a block diagram over a first embodiment implementing an arrangement according to the invention in a computer unit,

Fig. 4 is a schematic side-view of a mobile communication unit provided with an arrangement according to the invention, and

Fig. 5 is a block diagram showing another aspect of the invention.

DETAILED DESCRIPTION OF PREFERRED EMBODIMENT

The device 10, according to the invention, which is schematically shown in Fig.1, consists

mainly of two units denoted with 11 and 12.

The first unit consists of a sensor or a key part 10 for entering an identity, which performs an identification of the user. The key part 10 may be divided in two units: an input unit 13 and a key unit 14, which are preferably, but not necessarily, integrated in one physical unit 11.

Preferably, the input unit 13 may consist of any type of arrangement, preferably by means of which a unique identification information can be entered. A such arrangement may comprise a biometric sensor, PIN-code reader, voice detection device, eye detection device, card reader and so on, all well known for a skilled person.

The second part consists of a lock unit 12, protecting the object 15 in question.

The key unit 14 initiates a unique communication procedure between the key part 11 and the lock part 12. Unique for the invention is that the identification of the user is directly carried out in the key part 11 and do not occur in the lock part.

After registration of a user, a corresponding lock can be opened. There are two possibilities to open the lock, on one hand during a certain preselected time period, on the other hand permanently (if manually chosen), which however gives a poor safety. If the lock has been opened under a certain time period, the user is requested to identify himself once more when the time has lapsed.

Under the operation the identity is entered, e.g. by pressing the finger on a sensor (FPS), entering a pine code etcetera. If the identification of the user is approved, an encrypted electronical message from the key unit to the lock unit is sent, whereby the locked resource or object 15 (e.g. a hard disc in a computer) is made available for the user.

Using a secure transferring method between the units guarantees that it is not possible to send a false message to the lock unit for procuring access to the locked unit.

The external unit, the key unit 14, is provided with electronics, mainly including a microprocessor 16 with a built-in and substantially protected program and data memory.

The latter is a precaution, enabling access to the program or stored key information for reading or copying.

Preferably, there is a list of allowed users stored in the key unit 14. Maintenance of this register, such as adding new approved users, deletion of users etc., is carried out locally without communication with other units.

The key unit decides at every occasion, if the object should be protected, should be opened or locked. The decision is normally based on an operator/user decision, i.e. the key is initiated with allowed users. The locking may also occur on initiative of the lock unit after a certain predetermined time, if the operator despite a request, do not identify itself within a certain time.

The key unit can be completely open and must not be protected against infringement, since the computer and data store cannot be externally read outside the processor (security function in the processor).

The lock unit 12, which communicates with the key unit, e.g. via a serial connection, is mounted and protected on or in the object 15 to be locked. At each attempt to access the locked object by bypassing the normal login procedure through the key part 11 will be discovered by the lock unit. Alternative steps may be initiated, i.e. inactivity for a longer time period, warning messages, erasing data on a hard disc/storage unit etcetera.

The communication between the key and the lock units is carried out by means of, e.g. digitally coded signals via a serial connection.

The connection may be asynchronous and may occur with a relatively high transfer rate. The communication occurs with a special lock protocol, which may also comprise known parity and time controls.

As mentioned, the purpose with the safety system, according to the invention, is amongst others to prevent unauthorized access to, for instance computers, or more specifically, access to a certain hard disc and the information therein. To obtain an almost complete

security, an encrypted protocol can be used in the communication between the key part 11 and the lock part 12. The probability for successful infringement depends on the length of the random number, the protected length of the key and the length of the response. It may easily be made less than, for instance 10^{-18}, which practically means that it is safe for unauthorized access.

The lock protocol is a communication procedure ensuring computer integrity of the transmission and, guarantees that unauthorized infringement of the data exchange between the units cannot occur. If the message exchange is carried out correctly, the locked object is opened and stays open, respectively. If any errors should be detected, the object is locked.

For verifying authentication, the following message exchange may be used (see fig.2):

a. The key unit or the key code 14 starts a verification sequence by sending a request to the lock unit,

b. The lock unit responds with a variable random generated message,

c. At the same time a numerical value is calculated using a special algorithm utilizing a protected key. This value, which is completely derived from the response message sent out, is stored for later use,

d. The key unit responses with a numerical value being calculated from the received message using the same algorithm and key being used in the lock unit. This number may be used unchanged in the response, or coded in such a way that the lock unit can interpret it. If the lock unit receives a message, which contains a number being identical to, the number calculated at the transmission during step b, the authentication is considered as confirmed.

If the message exchange turns out correctly, according to steps a-d above, the locked object is unlocked, or remains open, respectively. If the response does not agree, the object remains locked.

The hidden key code may differ between the key and the lock unit (s) and between the lock units. This is possible because the key unit is initiated with additional information being specific for the connected lock unit, respectively. This enables the lock unit to return a correct response to the lock unit (as if it has access to the key code of the lock unit).

In the most preferred embodiment, a biometric sensor unit is used as the input unit.

Biometric sensors involve considerable advantages for identification of persons at entrance, computer access etc. Amongst the advantages, the speed can be mentioned, an extremely high degree of security for the identification and also above all no problems with forgotten passwords or password, which have fallen into the wrong hands. In combination with the invention, the sensor part performs a biometric identification of the fingerprints of the user. When the identification of the fingerprints of the user is approved, an encrypted message is sent from the key unit to the lock unit, whereby the locked resource is made available to the user.

Registers of allowed fingerprints are in the key unit. Maintenance of this register, i.e. adding new approved fingerprints, removing fingerprints etc., is done locally without any communication with other units.

The sensor unit may be provided with indication means, such as two light-emitting diodes, a red one and a green one, for facilitating registration and deregistration of fingerprints. The diodes indicate whether the lock is closed or opened, and also the status at the registration/removal of fingerprints.

In the following a number of non-limiting examples are given, which clarify different aspects of the invention.

The first non-limiting example, shown in fig. 3, relates to a hard disc unit 30 (or another memory unit or storage unit) in a computer unit provided with a fingerprint sensor 31 or a biometric sensor, i.e. an add-on unit. An add-on is one of many applications of the lock system according to the invention. With an add-on unit is meant a standard unit, such as a hard disc, which has been provided with a lock unit and which is connected to a computer unit (or the like) via a special electrical arrangement, which are located on, for instance a controller board 32 (insert card to the computer, such as ISA, PCI or the like). The electronic comprises of the key unit and also applications for communication with the soft ware in the computer via said data bus. To the board 32, a sensor 31 or alternatively other

identification equipment is connected directly or via, e.g. IR or radio (Bluetooth) or the like.

In this preferred embodiment, a standard hard disc is modified to work together with the lock device according to the invention. This implies that it is provided with an internally mounted lock system and which is through hardware prevents the disc from accessing data. An appropriate procedure depends on the unit (disc) construction.

Connections to the unit remain the same as to an ordinary hard disc, i.e. signal cables and a power feed from the power unit of the computer. An additional connection for the communication of the lock with the controller is provided.

Lock-functions, according to the invention, are obtained by means of the key unit and lock unit, respectively. The fingerprint sensor is connected through a cable and switch to the interface of the controller unit, on which the key unit is applied. The lock unit is arranged on the hard disc.

Except for lock functions, electronics for the communication with the programs of the computer are arranged in the lock unit. The program may amongst others pre-warn about the locking of the hard disc. Moreover, the locking can be carried out from the software.

To restart the computer a switch is used, normally mounted on the front side. This is always energised (Vin=+5 V), even when the computer is shut off, provided that the mains voltage is switched on. When switched, a signal is provided to the motherboard and the computer is started. By using the fingerprint sensor, the switch can be disconnected and Vin, which is through the contact, is instead connected to the controller card. From there it is connected further to the fingerprint sensor. In this way the fingerprint sensor is always switched on. An approved log in gives a signal from the controller card to the motherboard replacing the ordinary button pressing.

Locking may be initiated in several ways:

- Automatically, when a certain amount of time has passed (e.g. in case of unauthorized manipulation)
- When the user locks via the locking system.

- When the user locks with using a monitoring procedure, described below.

Unlocking can normally be carried out in one way, namely by providing a correct fingerprint.

If the person/persons who has/have registered their fingerprint/s is/are not available when the disc must be unlocked, there is a possibility for, e.g. the system manager or the security responsible unlock the unit by using an especial code. This must be a sufficiently complicated code to prevent practically any access.

An attempt made to force lock by providing false signals to the hard disc, may result in locking it for further access attempts, for instance during a certain time period or until a responsible person has reset the lock function.

The fingerprint sensor may also be completed with other locking devices, for instance smart cards.

With the exception for previously enumerated functions, the add-on unit is completely compatible with a standard hard disc.

For installation of an add-on unit, special software can be required. This will supervise the lock function via a controller card and indicate the status for the user. Particularly, the user must be warned in advance in good time before the disc is locked. With this program, it is also possible to directly lock the unit. Suitably, the program is always active and the status of the disc is shown in the system tray (activity field), where also different commands can be given.

Other application areas for the system, according to the invention, are for "Notebooks/Laptops", i.e. portable computers, where all types of storing media are secured, HDD, FDD, CD, RAM, ROM, flash memory, main controller board comprising all the components such as BIOS, controller units for controlling data media etcetera.

In stationary computers/servers, the protection of the components on network cards and the like for administration of networks can be applied.

The system may be arranged as a remote control combined with a mobile telephone, as a code-provider unit. Data code generator for non-recurrent codes for accesses to computers, alarm systems, car locks, passage systems etcetera.

Transaction codes via telephone systems, GSM, WAP or the like may occur. The unit, according to the invention, unlocks the unit and after that it is possible to choose the type of action.

In an application using the invention for bank transactions or the like via, e.g. a computer, the client may be provided with a sensor/key unit according to the invention. The client unit is provided with an embedded unique pin-code and a special algorithm. The pin-code may be of the type being used at credit or bankcard applications, but slightly more advanced. The same pin-code can also be stored in the key unit being used by the client. The pin-code may be changed by means of special terminals on the bank. The same unique code can be associated with the account number of the client.

In the bank, when a transaction request is received a response is generated by means of a special calculation unit, which proves that the request from the correct key unit is authentic belonging to the right account holder.

The function may be described in more detail, according to the following steps:

- the client contacts the bank by means of a computer program installed in his computer and enters his account number,
- the bank issues a reply comprising an identification part, lock-data and so on,
- the client selects the type of transaction and fills in the amount and so on and verifies the transaction,
- the program transmits a locking transaction, according to the above description, and also transaction data comprising, for instance amount, account number, time stamp and so on,
- a reply is received only if the lock unit has received the right identification from the key unit; the response may comprise identity, variable locking/unlocking data and also transaction data, and is sent to the bank. The transaction data (for instance the

sum) and authentication of the performer of the transaction is verified at the same time.

- the bank uses the algorithm, as mentioned before, together with the pin-code of the client for verifying the response, and if correct response can be urged of the incoming responses and transaction data, which assures that nothing has been changed after the biometry control, the transaction is accepted and the client is informed.

If the trade or transaction is carried out, for instance over Internet, the user may be provided with a key unit arranged with, for instance a biometric sensor or the like. The key unit of the user is provided with a unique identification in form of a check sum or the like. The same unique identification can be associated with the accounting number of the user at the bank. The bank is arranged with controlling means for verification of correct transaction request in the same way as above. In this case, the verification and the transaction are first performed by the bank and then to the seller, in the same way as above.

In one further example, the invention is used in a mobile unit, such as a mobile telephone, shown in Fig. 4. The security arrangement 40 consists of two relative each other pivoting parts 41 and 42 (according to this example), where the part 42 comprises a connector 43 for connection to the communication port (not shown) of the telephone 44. The device comprises a sensor unit 45, such as a biometric sensor and the like and corresponding electronics and memory arranged on the second part 41. The electronics can be powered by the power source of the telephone. The connection part is connected to the telephone and the sensor part 41 is attached onto the backside of the telephone, for instance over its battery. When connected, the telephone can be used as a control or key unit, according to the above description.

The telephone can only be accessed if the right person verified via the sensor uses the telephone, which also can be used for controlling other units, for instance when payments over the telephone network, remote controlling, opening doors, access to computers (for instance via the IR interface), etc. In this case the lock unit can be implemented in the telephone.

Examples of other applications employing the invention include:

- Radio add-on (RFR), i.e., a memory unit, for instance a hard disc, provided with a biometric or transponder card reader.
- Lock unit for portable equipment (hand-held computers), only operating when a certain transponder is in the vicinity. The transponder can for instance be built in the wristwatch. In addition, the wristwatch may be provided with a biometric sensor communicating with the hand-held computer via IR or RF.
- The lock device may be built inside a remote control for ensuring that only one authorized user can obtain access to the remote-controlled equipment.
- When encrypting/decrypting, i.e. e-mails or files, encryption can be carried out by means of a public key while decryption by means of a private key being verified with regard to the right person using a biometric sensor.

The invention is not limited to use of a key or lock unit, but combinations of several key and lock units where one or several key/lock units cooperate may also occur. The block diagram in figure 5 shows such arrangement, in which L_1-L_5 denote lock units and K_1 and K_2 denote key units. A key unit, for instance K_1 may be arranged to open a number of lock units, for instance L_1-L_4, while K_2 opens L_4 and L_5. The term open means also access to different resources and information. The communication between lock units and between lock units and key units can be carried out via radio, Internet (or other networks), IR and so on, preferably decrypted according to the description above.

While we have illustrated and described only preferred embodiments of the invention, it is realized that several variations and modifications within the scope of the enclosed claims can occur.

CLAIMS

1. Security arrangement (10) for ensuring access to a unit or information in a unit, mainly comprising a key unit (11) and a lock unit (12),
characterised in,
that the key unit (11) is arranged in a distance from the lock unit comprising an input unit (13) and a communication unit (14), and that identification of a user is performed in the key unit (11) before the key unit accepts locking/unlocking.

2. Arrangement as claimed in claim 1,
characterised in,
that the said unit is a computer, cash dispenser, door lock, car door, remote control, mobile communication unit, portable computer and the like.

3. Arrangement as claimed in claim 1 or 2,
characterised in,
that the input unit is a biometric sensor, PIN code reader, voice detection device, eye detection device, card reader or mobile telephone and so on.

4. Arrangement as claimed in claim 1 - 3,
characterised in,
that the user identity is stored in the key unit.

5. Arrangement as claimed in claim 1 - 4,
characterised in,
that the key unit communicates with the lock unit by:

a. starting a verification sequence by the key unit by sending a request to the lock unit,

b. the lock unit responding with a variable, substantially randomly generated message,

c. calculating a numerical value by means of an algorithm using a protected key, which value is completely derived from the transmitted response message,

d. responding with a numerical value being calculated from the received message using said algorithm and key, which are used in the lock unit, and if the lock unit receives

a message containing a value being identical to the value calculated during the transmission under step b, the authentication is confirmed.

6. Arrangement as claimed in claim 5,
characterised in
that said value can be used unchanged in the response, or encrypted in such a way that the lock unit can interpret it.

7. Security arrangement for a memory unit (30) in a computer unit provided with a biometric sensor (31),
characterised in
that the memory unit is provided with an internally mounted lock system, which as a hardware prevents access to data and is connected to the computer unit via a controller unit (32), which is comprises a key unit and also functions for communication with parts in the computer unit via said controller unit, directly or via a link connected to said sensor (31) or other alternative identification equipment.

8. Security arrangement as claimed in claim 7,
characterised in,
that said controller unit is an ISA card, PCI card or the like.

9. Security arrangement as claimed in claim 7 or 8,
characterised in,
that the controller unit comprises the key unit.

10. Security arrangement as claimed in claim 7 - 9,
characterised in,
that the computer unit is started through said sensor via the controller unit.

11. Security arrangement as claimed in claim 7 - 10,
characterised in,
that the locking can be initiated in several ways: automatically, after that a certain time has lapsed and/or by the user via the lock system, and/or by a user using a security procedure.

12. A mobile communication unit (44) provided with a security arrangement (40) for ensuring acquisition to a unit or information in a unit,
characterised in,
that the security arrangement is an external unit connected to a communication port of the communication unit, that the arrangement is provided with a biometric sensor being connected to the communication unit, whereby the communication unit constitute one of a key unit and/or a lock unit, and that identification of a user is executed in the lock unit before locking/unlocking is accepted by the lock unit.

13. Method in a security arrangement (10) for ensuring access to a unit or information in a unit, substantially comprising a key unit (11) and a lock unit (12),
characterised by
arranging the key unit (11) distanced from the lock unit comprising an input unit (13) and a communication unit (14), and identifying a user in the key unit (11) before locking/unlocking accepted by the key unit.

14. Method as claimed in claim 13,
comprising verification of the authentication steps of:

a. initiating a verification by the key unit by sending a request to the lock unit,

b. responding by the lock unit with a varying, randomly generated message,

c. calculating a numerical value simultaneously by means of a special algorithm using a protected key and storing it for later use,

d. responding by the key unit with a numerical value being calculated from the message received, using the same algorithm and key used in the lock unit, and

e. confirming authentication if the lock unit receives a message containing a numerical value, which is identical to the one confirmed at the transmission during step b.

15. Method as claimed in claim 14,
characterised in
that said value is completely derived from the response message.

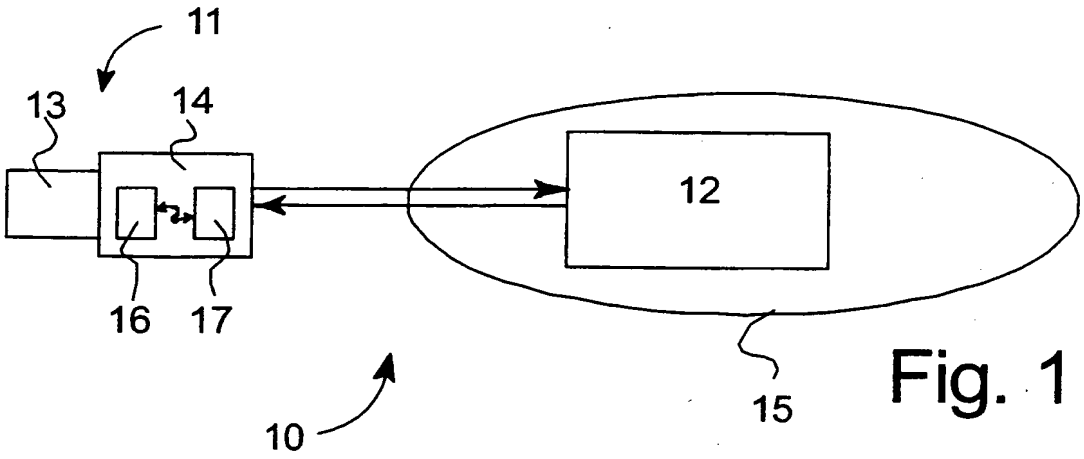


Fig. 1

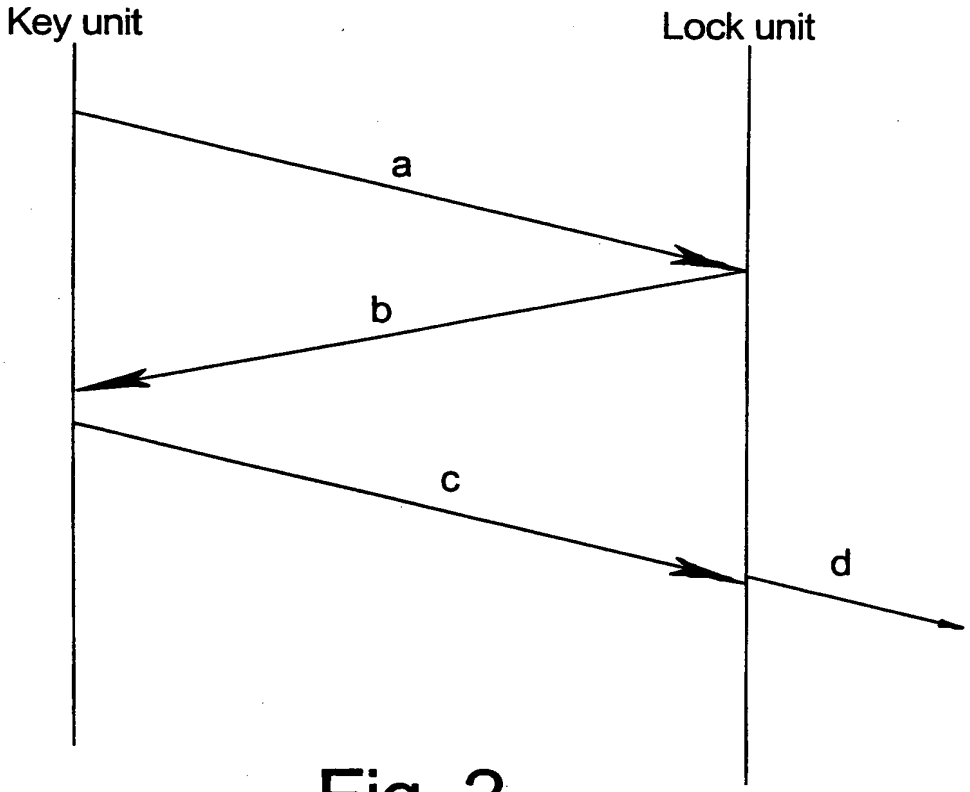


Fig. 2

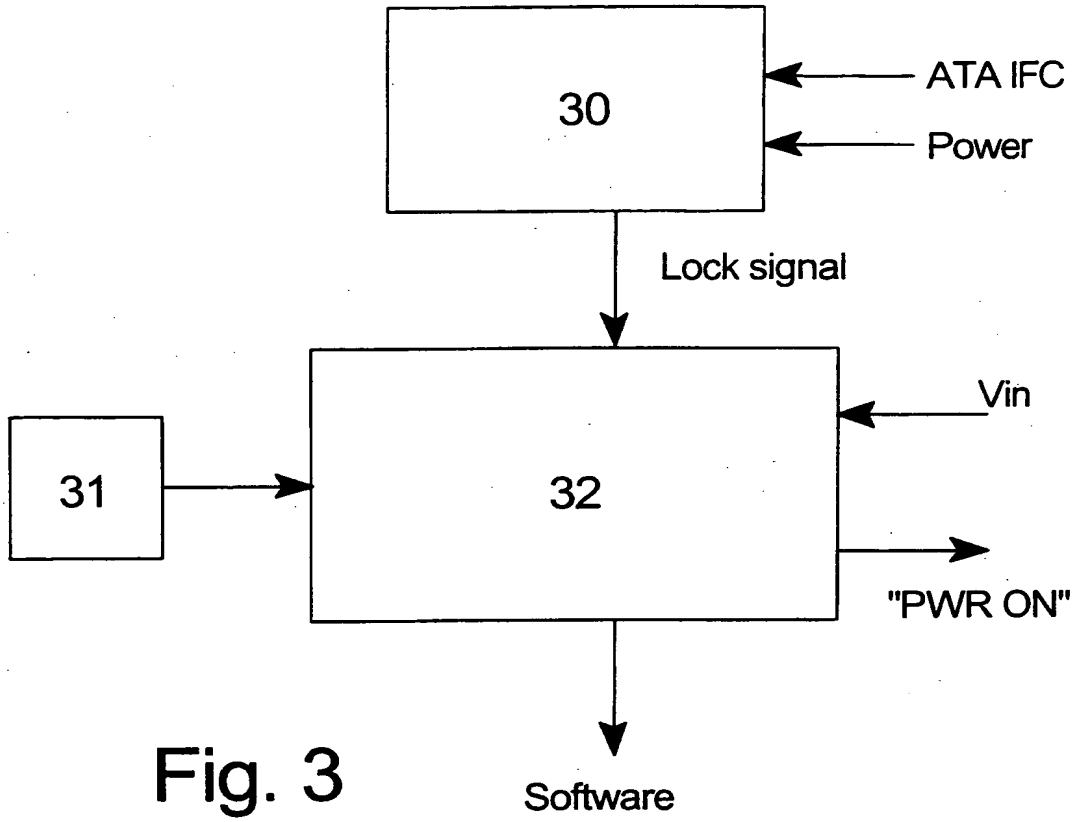


Fig. 3

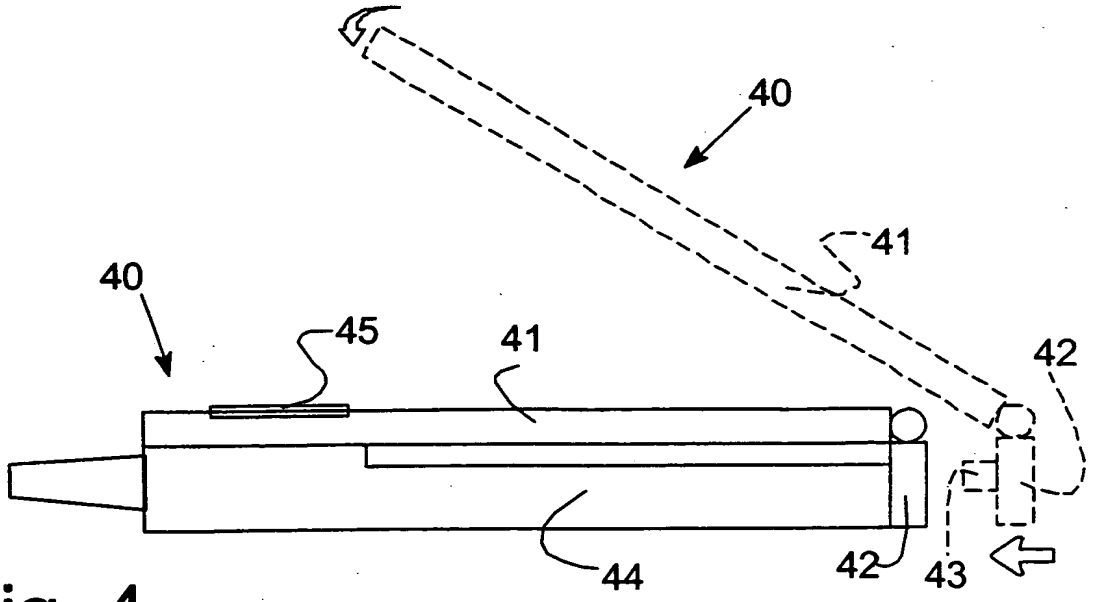


Fig. 4

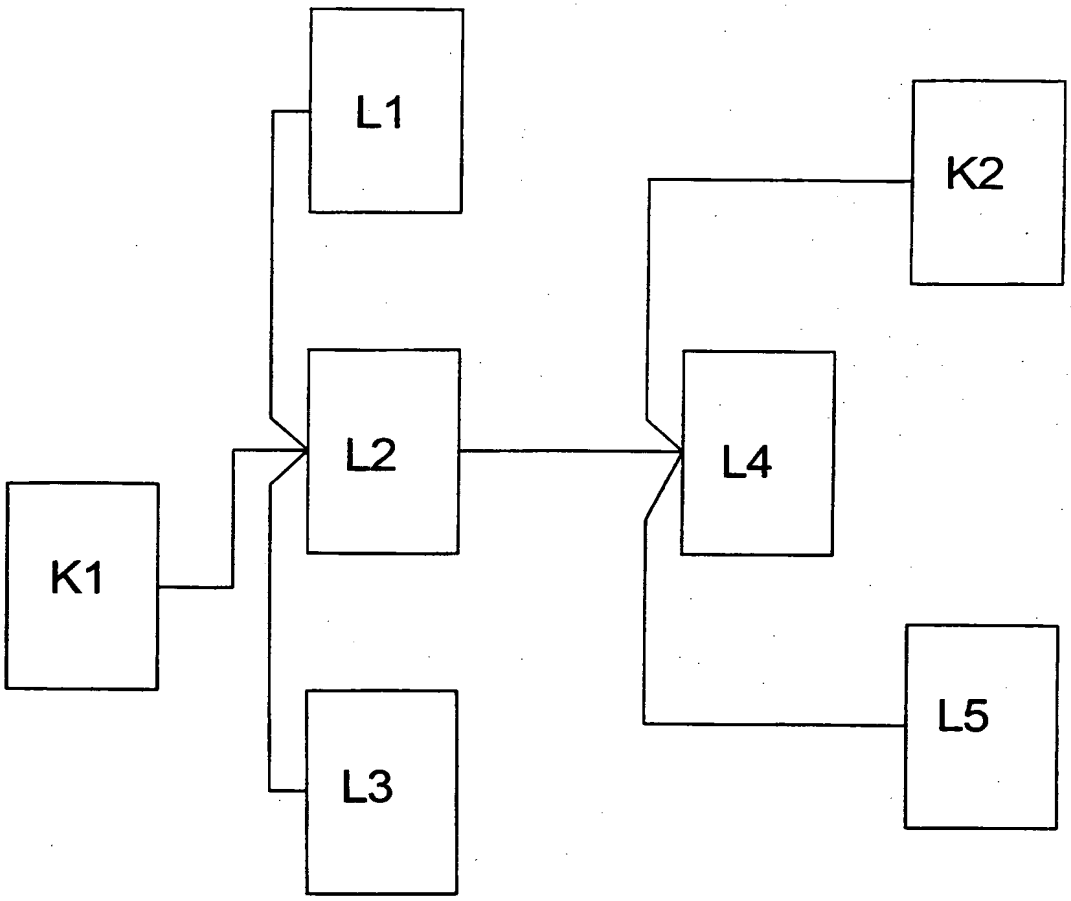


Fig. 5

INTERNATIONAL SEARCH REPORT

International application No.
PCT/SE 00/01811

A. CLASSIFICATION OF SUBJECT MATTER

IPC7: G06F 12/14, G06F 1/00, H04L 29/06
According to International Patent Classification (IPC) or to both national classification and IPC

B. FIELDS SEARCHED

Minimum documentation searched (classification system followed by classification symbols)

IPC7: G06F, H04L

Documentation searched other than minimum documentation to the extent that such documents are included in the fields searched

SE,DK,FI,NO classes as above

Electronic data base consulted during the international search (name of data base and, where practicable, search terms used)

C. DOCUMENTS CONSIDERED TO BE RELEVANT

Category*	Citation of document, with indication, where appropriate, of the relevant passages	Relevant to claim No.
X	US 5757918 A (HOPKINS), 26 May 1998 (26.05.98), column 2, line 18 - line 23; column 3, line 25 - line 38; column 6, line 6 - line 10, column 9, line 13 - line 29, abstract --	1-15
X	US 5668876 A (FALK ET AL.), 16 Sept 1997 (16.09.97), column 1, line 65 - column 2, line 48, claims 1,7,19,20,32-33, abstract --	1-15
X	US 5280527 A (GULLMAN ET AL.), 18 January 1994 (18.01.94), column 2, line 20 - column 3, line 5; column 5, line 11 - line 33; column 5, line 41 - line 54, claims 4,10, abstract --	1-15

[X] Further documents are listed in the continuation of Box C. [X] See patent family annex.

* Special categories of cited documents:
"A" document defining the general state of the art which is not considered to be of particular relevance
"E" earlier application or patent but published on or after the international filing date
"L" document which may throw doubts on priority claim(s) or which is cited to establish the publication date of another citation or other special reason (as specified)
"O" document referring to an oral disclosure, use, exhibition or other means
"P" document published prior to the international filing date but later than the priority date claimed
"T" later document published after the international filing date or priority date and not in conflict with the application but cited to understand the principle or theory underlying the invention
"X" document of particular relevance: the claimed invention cannot be considered novel or cannot be considered to involve an inventive step when the document is taken alone
"Y" document of particular relevance: the claimed invention cannot be considered to involve an inventive step when the document is combined with one or more other such documents, such combination being obvious to a person skilled in the art
"&" document member of the same patent family

Date of the actual completion of the international search	Date of mailing of the international search report
12 December 2000	08-01-2001
Name and mailing address of the ISA/ Swedish Patent Office Box 5055, S-102 42 STOCKHOLM Facsimile No. +46 8 666 02 86	Authorized officer Per Heimdal Telephone No. +46 8 782 25 00

INTERNATIONAL SEARCH REPORT

International application No.
PCT/SE 00/01811

C (Continuation). DOCUMENTS CONSIDERED TO BE RELEVANT

Category*	Citation of document, with indication, where appropriate, of the relevant passages	Relevant to claim No.
X	WO 9934554 A2 (KONINKLIJKE PHILIPS ELECTRONICS N.V.), 8 July 1999 (08.07.99), page 3, line 15 - page 6, line 32; page 9, line 16 - page 10, line 20, claim 1	1-15
	--	
X	WO 9939310 A1 (PHELPS, BARRY, C.), 5 August 1999 (05.08.99), page 6, line 29 - page 7, line 27, abstract	1-15
	--	
X	EP 0924656 A2 (TRW INC.), 23 June 1999 (23.06.99), column 1, line 55 - column 4, line 38, figure 4, abstract	1-15
	--	
X	WO 9812670 A1 (DEW ENGINEERING AND DEVELOPMENT LIMITED), 26 March 1998 (26.03.98), page 3, line 1 - page 6, line 27; page 8, line 19 - page 9, line 2; page 11, line 16 - line 21, page 15, line 20 - line 25, page 16, line 24 - line 27, page 19, line 7 - line 13	1-15
	--	

INTERNATIONAL SEARCH REPORT

International application No.
PCT/SE00/01811

Box I Observations where certain claims were found unsearchable (Continuation of item 1 of first sheet)

This international search report has not been established in respect of certain claims under Article 17(2)(a) for the following reasons:

1. ☐ Claims Nos.:
because they relate to subject matter not required to be searched by this Authority, namely:

2. ☐ Claims Nos.:
because they relate to parts of the international application that do not comply with the prescribed requirements to such an extent that no meaningful international search can be carried out, specifically:

3. ☐ Claims Nos.:
because they are dependent claims and are not drafted in accordance with the second and third sentences of Rule 6.4(a).

Box II Observations where unity of invention is lacking (Continuation of item 2 of first sheet)

This International Searching Authority found multiple inventions in this international application, as follows:

Invention I: Claims 1-6 and 12-15.

Invention II: Claims 7-11.

1. ☐ As all required additional search fees were timely paid by the applicant, this international search report covers all searchable claims.
2. ☒ As all searchable claims could be searched without effort justifying an additional fee, this Authority did not invite payment of any additional fee.
3. ☐ As only some of the required additional search fees were timely paid by the applicant, this international search report covers only those claims for which fees were paid, specifically claims Nos.:

4. ☐ No required additional search fees were timely paid by the applicant. Consequently, this international search report is restricted to the invention first mentioned in the claims: it is covered by claims Nos.:

Remark on Protest

☐ The additional search fees were accompanied by the applicant's protest.

☐ No protest accompanied the payment of additional search fees.

INTERNATIONAL SEARCH REPORT

Information on patent family members

04/12/00

International application No.
PCT/SE 00/01811

Patent document cited in search report	Publication date	Patent family member(s)	Publication date
US 5757918 A	26/05/98	CA 2167631 A	21/07/96
		EP 0723251 A	24/07/96
US 5668876 A	16/09/97	AU 692881 B	18/06/98
		AU 2688795 A	19/01/96
		CA 2193819 A	04/01/96
		EP 0766902 A	09/04/97
		FI 965161 A	13/02/97
		JP 10502195 T	24/02/98
		WO 9600485 A	04/01/96
US 5280527 A	18/01/94	CA 2105404 A	03/03/95
WO 9934554 A2	08/07/99	CN 1252198 T	03/05/00
		EP 0962070 A	08/12/99
WO 9939310 A1	05/08/99	AU 2345499 A	16/08/99
		GB 2340274 A	16/02/00
		GB 9909897 D	00/00/00
		JP 3096457 B	10/10/00
		JP 2000040002 A	08/02/00
		US 6108712 A	22/08/00
EP 0924656 A2	23/06/99	JP 11265432 A	28/09/99
		US 6041410 A	21/03/00
WO 9812670 A1	26/03/98	AU 4196497 A	14/04/98
		CA 2233942 A	26/03/98

(12) INTERNATIONAL APPLICATION PUBLISHED UNDER THE PATENT COOPERATION TREATY (PCT)

(19) World Intellectual Property Organization
International Bureau

(43) International Publication Date
22 March 2001 (22.03.2001)

PCT

(10) International Publication Number
WO 01/20463 A1

(51) International Patent Classification[7]: G06F 12/14, 1/00, H04L 29/06

(21) International Application Number: PCT/SE00/01811

(22) International Filing Date:
18 September 2000 (18.09.2000)

(25) Filing Language: Swedish

(26) Publication Language: English

(30) Priority Data:
60/154,395 17 September 1999 (17.09.1999) US
0001687-3 5 May 2000 (05.05.2000) SE

(71) Applicant *(for all designated States except US)*: FINGLOQ AB [SE/SE]; Banehagsliden 5, S-414 51 Göteborg (SE).

(72) Inventors; and
(75) Inventors/Applicants *(for US only)*: MARTINSSON, Roy [SE/SE]; Laxgatan 1D, S-426 79 Västra Frölunda (SE). ANDLER, Oskar [SE/SE]; Furugatan 1, S-413 21 Göteborg (SE).

(74) Agent: GÖTEBORGS PATENTBYRÅ DAHLS AB; Sjöporten 4, S-417 64 Göteborg (SE).

(81) Designated States *(national)*: AE, AG, AL, AM, AT, AT (utility model), AU, AZ, BA, BB, BG, BR, BY, BZ, CA, CH, CN, CR, CU, CZ, CZ (utility model), DE, DE (utility model), DK, DK (utility model), DM, DZ, EE, EE (utility model), ES, FI, FI (utility model), GB, GD, GE, GH, GM, HR, HU, ID, IL, IN, IS, JP, KE, KG, KP, KR, KR (utility model), KZ, LC, LK, LR, LS, LT, LU, LV, MA, MD, MG, MK, MN, MW, MX, MZ, NO, NZ, PL, PT, RO, RU, SD, SE, SG, SI, SK, SK (utility model), SL, TJ, TM, TR, TT, TZ, UA, UG, US, UZ, VN, YU, ZA, ZW.

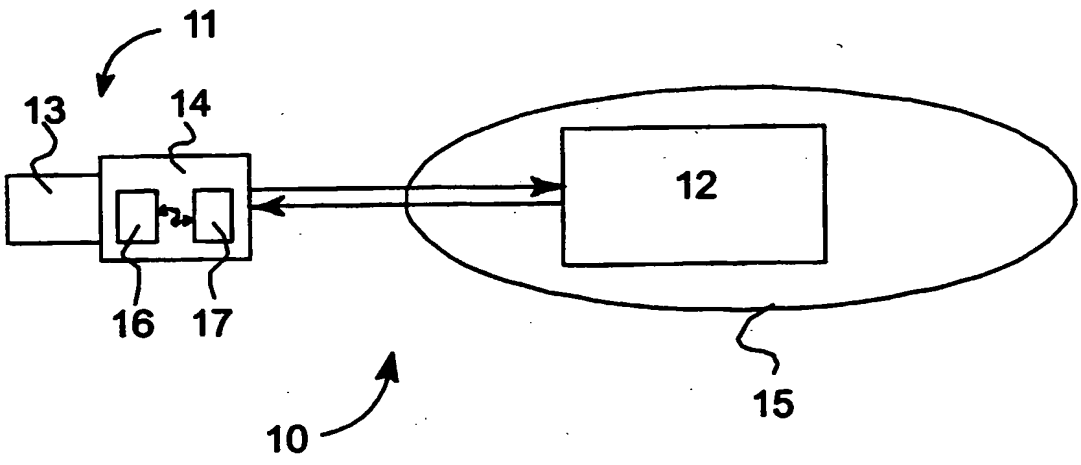
(84) Designated States *(regional)*: ARIPO patent (GH, GM, KE, LS, MW, MZ, SD, SL, SZ, TZ, UG, ZW), Eurasian patent (AM, AZ, BY, KG, KZ, MD, RU, TJ, TM), European patent (AT, BE, CH, CY, DE, DK, ES, FI, FR, GB, GR, IE, IT, LU, MC, NL, PT, SE), OAPI patent (BF, BJ, CF, CG, CI, CM, GA, GN, GW, ML, MR, NE, SN, TD, TG).

Published:
— *With international search report.*
— *With amended claims.*

Date of publication of the amended claims: 10 May 2001

For two-letter codes and other abbreviations, refer to the "Guidance Notes on Codes and Abbreviations" appearing at the beginning of each regular issue of the PCT Gazette.

(54) Title: SECURITY ARRANGEMENT



(57) Abstract: The present invention relates to a security arrangement (10) for ensuring access to a unit or information in a unit, mainly comprising a key unit (11) and a lock unit (12). The key unit (11) is arranged in a distance from the lock unit comprising an input unit (13) and a communication unit (14). The identification of a user is performed in the key unit (11) before the lock unit accepts locking/unlocking.

WO 01/20463 A1

AMENDED CLAIMS

[received by the International Bureau on 31 July 2000 (31.07.00);
original claims 1-15 replaced by new claims 1-13 (3 pages)]

1. Security arrangement (10) for ensuring access to a unit or information in a unit by authenticating a user, said arrangement mainly comprising a key unit (11) and a lock unit (12), the key unit (11) being arranged distanced from said lock unit comprising an input unit (13) and a communication unit (14), whereby the authentication of the user is performed in the key unit (11) before the key unit accepts locking/unlocking of said lock unit,
characterised in
that the key unit is arranged to communicate with the lock unit by starting a verification sequence by sending a request to said lock unit, the lock unit is arranged to respond by transmitting a variable, substantially randomly generated message, and to calculate a numerical value by means of an algorithm using a protected key, which numerical value is derived from the transmitted response message, and said key unit is arranged to respond with a numerical value being calculated from the received message using said algorithm and said protected key, and if said lock unit receives a message containing a value being identical to the value calculated by the lock unit, the authentication is confirmed.

2. Arrangement as claimed in claim 1,
characterised in
that the said unit is a computer, cash dispenser, door lock, car door, remote control, mobile communication unit, portable computer and the like.

3. Arrangement as claimed in claim 1 or 2,
characterised in
that the input unit is a biometric sensor, PIN code reader, voice detection device, eye detection device, card reader or mobile telephone and so on.

4. Arrangement as claimed in claim 1 - 3,
characterised in
that the user identity is stored in the key unit.

5. Arrangement as claimed in claim 1,

characterised in

that said value can be used unchanged in the response, or encrypted in such a way that the lock unit can interpret it.

6. Security arrangement according to claim 1,
characterised in
that it is provided for a memory unit (30) in a computer unit,
that said key unit is a biometric sensor (31),
that the lock unit is provided within the memory unit, which prevents access to data and is connected to the computer unit via a controller unit (32).

7. Security arrangement as claimed in claim 6,
characterised in
that said controller unit is an ISA card, PCI card or the like.

8. Security arrangement as claimed in claim 6 or 7,
characterised in
that the controller unit comprises the key unit.

9. Security arrangement as claimed in claim 6 - 8,
characterised in
that the computer unit is started through said sensor via the controller unit.

10. Security arrangement as claimed in claim 6 - 9,
characterised in
that the locking can be initiated in several ways: automatically, after that a certain time has lapsed and/or by the user via the lock system, and/or by a user using a security procedure.

11. A mobile communication unit (44) provided with a security arrangement (40) according to claim 1 for ensuring acquisition to a unit or information in a unit,
characterised in,
that the security arrangement is an external unit connected to a communication port of the communication unit, that the arrangement is provided with a biometric sensor being

connected to the communication unit, whereby the communication unit constitute one of a key unit and/or a lock unit, and that identification of a user is executed in the lock unit before locking/unlocking is accepted by the lock unit.

12. Method of authentication in a security arrangement (10) for ensuring access to a unit or information in a unit, substantially comprising a key unit (11) and a lock unit (12), the key unit (11) is arranged distanced from the lock unit comprising an input unit (13) and a communication unit (14),
characterised by the steps of:

a. initiating a verification by the key unit by sending a request to the lock unit,

b. responding by the lock unit with a varying, randomly generated message,

c. calculating a numerical value simultaneously by means of a special algorithm using a protected key and storing it for later use,

d. responding by the key unit with a numerical value being calculated from the message received, using the same algorithm and key used in the lock unit, and

e. confirming authentication if the lock unit receives a message containing a numerical value, which is identical to the one confirmed at the transmission during step b.

13. Method as claimed in claim 12,
characterised in
that said value is completely derived from the response message.